

Symantec™ Endpoint Protection 14.2.2 Release Notes

Symantec Endpoint Protection Release Notes

Product version: 14.2.2

Documentation version: 1

This document was last updated on: November 12, 2019

Legal Notice

Copyright © 2019 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Symantec Support

Knowledge Base articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

<https://support.symantec.com/>

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

<https://www.symantec.com/connect/>

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

Before you contact Symantec Support, see: <https://entced.symantec.com/default/ent/supportref>

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Release notes

This document includes the following topics:

- [About this document](#)
- [What's new for 14.2 RU2 \(14.2.2\)](#)
- [Known issues and workarounds](#)
- [System requirements for Symantec Endpoint Protection](#)
- [Supported upgrade paths to Symantec Endpoint Protection](#)
- [Where to get more information](#)

About this document

This document contains information for Symantec Endpoint Protection.

Review this document before you install the product or before you call Technical Support. The release notes describe known issues and their workarounds that are not included in the standard documentation or online Help.

See [“Known issues and workarounds”](#) on page 5.

See [“System requirements for Symantec Endpoint Protection”](#) on page 7.

What's new for 14.2 RU2 (14.2.2)

- Added the following operating system support:
 - Windows 10 19H2 (version 1909)
 - macOS 10.15 (Catalina)
- Upgraded multiple third-party components to newer versions.

[What's new in all releases of Symantec Endpoint Protection](#)

See [“Known issues and workarounds”](#) on page 5.

Known issues and workarounds

The items in this section apply to this release of Symantec Endpoint Protection.

- See [“Upgrade information”](#) on page 5.
- See [“Client information”](#) on page 5.
- See [“Symantec Endpoint Protection Manager information”](#) on page 7.

You can view a list of resolved issues for this release at the following location:

[New fixes and component versions in Symantec Endpoint Protection 14.2 RU2](#)

Upgrade information

This section contains information about upgrading to the current release of the product.

Custom names may prevent the firewall policy from updating during an upgrade to 14.2 or later

For an upgrade to Symantec Endpoint Protection 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if you changed some default names. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected.

If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add.

Client information

This section contains information about the Symantec Endpoint Protection client for Windows, Mac, or Linux.

Mac clients that enable WSS Traffic Redirection do not honor custom proxy settings for LiveUpdate

You have configured your managed Mac clients for Symantec Endpoint Protection 14.2 RU1 MP1 to use custom proxy settings for LiveUpdate through External Communications Settings. After you enable WSS Traffic Redirection (WTR) for your Mac clients through the Symantec

Endpoint Protection Manager policy, however, you find that LiveUpdate traffic no longer honors your custom proxy settings. Instead, LiveUpdate attempts a direct connection.

To work around this issue, only use custom proxy settings for LiveUpdate when WSS Traffic Redirection is disabled.

Symantec Endpoint Protection feature Endpoint Threat Detection for Active Directory (SETDAD) does not add a remote DM

Symantec Endpoint Protection fails to add a new remote DM for a domain that is not trusted on the SETDAD computer domain.

To work around this issue, examine the account privileges on the remote DM computer in place of the SETDAD computer.

Symantec Endpoint Protection feature Endpoint Threat Detection for Active Directory does not make detections on its own core server

You install Symantec Endpoint Protection with the Symantec Endpoint Threat Detection for Active Directory feature on the following Endpoint Threat Detection for AD servers:

- Core server
- Deployment Manager server

The feature shows as enabled in Symantec Endpoint Protection Manager. However, the alerts for Endpoint Threat Defense for AD stop working for all clients.

Currently, you should not enable the Endpoint Threat Detection for AD feature when you install Symantec Endpoint Protection to either of these servers. You should also ensure that these servers are not in a group that has applied an Endpoint Threat Detection for AD policy to it.

This support is planned for a future release.

Symantec Endpoint Protection feature Endpoint Threat Detection for Active Directory does not load on a domain controller

You install Symantec Endpoint Protection with the Symantec Endpoint Threat Detection for Active Directory feature onto your domain controller. However, the agent for this feature does not load on the domain controller.

This behavior is working as designed. The agent for Endpoint Threat Detection for AD is not supported on domain controllers.

Microsoft Edge unexpectedly allows PDF downloads with Hardening enabled

With Hardening enabled in the Symantec Endpoint Protection client, you are unexpectedly able to download PDF files if you use the Microsoft Edge browser. The prevention of the download of PDF files works as expected with other browsers.

A fix for this issue is planned for a future release.

Symantec Endpoint Protection Manager information

This section contains information about Symantec Endpoint Protection Manager.

"Deployment in progress" still appears in Symantec Endpoint Protection Manager after the client receives an updated policy for Endpoint Threat Defense for AD

You apply a policy for Symantec Endpoint Threat Defense for Active Directory 3.3 to a group. This group contains some clients that run Symantec Endpoint Protection 14.2 RU1 or earlier. These clients receive and apply the policy as expected, but the status in Symantec Endpoint Protection Manager continues to show the message **Deployment in progress**.

This behavior is expected. Endpoint Threat Defense for AD 3.3 policies are only supported on the client as of version 14.2 RU1 MP1.

Remote Java Console access to Symantec Endpoint Protection Manager fails with FIPS enabled

In a FIPS-compliant environment, access to Symantec Endpoint Protection Manager 14.2 RU1 MP1 using the Java remote console fails with the error: "Failed to validate certificate. The application will not be executed." This error results from an incompatibility between Crypto-J and JRE 8. To work around this issue, access Symantec Endpoint Protection Manager using the web console.

[Remote Java Console access to Endpoint Protection Manager fails with FIPS enabled](#)

System requirements for Symantec Endpoint Protection

In general, the system requirements for the following are the same as those of the operating systems on which they are supported:

- Symantec Endpoint Protection Manager
- The Symantec Endpoint Protection clients

The system requirements for this release appear on the following pages:

- [System requirements for Symantec Endpoint Protection 14.2 RU2](#)
- [Supported virtual installations and virtualization products](#)
- [Internationalization requirements](#)

Supported upgrade paths to Symantec Endpoint Protection

Symantec Endpoint Protection Manager and Windows client

The following versions of Symantec Endpoint Protection Manager and Symantec Endpoint Protection Windows client can upgrade directly to 14.2 RU2 (14.2.2):

- 11.x and Small Business Edition 12.0 (Symantec Endpoint Protection clients only, for supported operating systems)
- 12.1.x, up to 12.1.6 MP10
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1

Mac client

The following versions of Symantec Endpoint Protection client for Mac can upgrade directly to 14.2 RU2 (14.2.2):

- 12.1.4 - 12.1.6 MP9
The Mac client did not update for version 12.1.6 MP10.
- 14
- 14 MP1

- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1

Note: The Symantec Endpoint Protection client for Mac was not updated for 14.0.1 MP2.

Linux client

The following versions of Symantec Endpoint Protection client for Linux can upgrade directly to 14.2 RU2 (14.2.2):

- 12.1.x, up to 12.1.6 MP9
The Linux client did not update for version 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1

Symantec AntiVirus for Linux 1.0.14 is the only version that you can migrate directly to Symantec Endpoint Protection. You must first uninstall all other versions of Symantec AntiVirus for Linux. You cannot migrate a managed client to an unmanaged client.

Unsupported upgrade paths

You cannot migrate to Symantec Endpoint Protection from all Symantec products. You must uninstall the following products before you install the Symantec Endpoint Protection client:

- The unsupported Symantec products Symantec AntiVirus and Symantec Client Security

- All Symantec Norton™ products
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Versions of Symantec Endpoint Protection for Mac earlier than 12.1.4

You cannot upgrade Symantec Endpoint Protection Manager 11.0.x or Symantec Endpoint Protection Manager Small Business Edition 12.0.x directly any version of Symantec Endpoint Protection Manager 14. You must first uninstall these versions or perform an upgrade to 12.1.x before an upgrade to 14.x.

Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.2.1.1 to 12.1.6 MP10, you must first uninstall Symantec Endpoint Protection 14.2.1.1.

If you have a build number but you are not sure how it translates to release version, see:

- [Released versions of Symantec Endpoint Protection](#)
- [About Endpoint Protection release types and versions](#)

Where to get more information

[Table 1-1](#) displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 1-1 Symantec website information

Types of information	Website link
Trial versions	Trialware
Manuals and documentation updates	English: ■ Symantec Product Documentation ■ Product guides for all versions of Symantec Endpoint Protection 14.x Other languages: ■ Brazilian Portuguese ■ Chinese (simplified) ■ Chinese (traditional) ■ French ■ German ■ Italian ■ Japanese ■ Korean ■ Spanish * Czech, Polish, and Russian files are on the English page.

Table 1-1 Symantec website information (*continued*)

Types of information	Website link
Technical Support	Endpoint Protection Technical Support Includes knowledge base articles, product release details, updates and patches, and contact options for support.
Threat information and updates	Symantec Security Center
Training	Symantec Education Services Access the training courses, the eLibrary, and more.
Symantec Connect forums	Endpoint Protection